

ALEXANDER KUGELMAN (SBN 255463)
Kugelman Law, P.C.
21 Tamal Vista Blvd., Suite 202
Corte Madera, CA 94925
Telephone: (415) 968-1780
Facsimile: (415) 534-9441
alex@kugelmanlaw.com

Attorney for Claimant
ILIJA MR. MATUSKO

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

Approximately 69,370 Bitcoin (BTC), Bitcoin
Gold (BTG), Bitcoin SV (BSV), and Bitcoin
Cash (BCH) seized from
1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx,

Defendant.

ILIJA MR. MATUSKO,

Claimant.

Case No. CV 20-7811 RS

**DECLARATION OF CHRISTOPHER
WAJDA IN SUPPORT OF CLAIMANT'S
OPPOSITION TO MOTION TO STRIKE
THE VERIFIED CLAIM OF ILIJA MR.
MATUSKO**

Date: September 30, 2021
Time: 1:30 pm
Cttrm: 3 (Via Zoom)

The Hon. Richard Seeborg

Trial Date: None Set

DECLARATION OF CHRISTOPHER WAJDA

I, CHRISTOPHER WAJDA, declare as follows:

1. I am currently the Managing Director of the Black Raven Advisory Group LLC, a niche firm that specializes in complex criminal and civil financial investigations. I am a retired Assistant Special Agent in Charge, Internal Revenue Service – Criminal Investigation (“IRS-CI”). I have over 32 years of experience with the Internal Revenue Service; 21 years as a Special Agent in the field and as a leader with IRS-CI focusing solely on criminal investigations related to white

1 collar criminal offenses with a specialty in federal tax crimes and money laundering violations.
2 My time as a leader in IRS-CI includes over 2 years as a Senior Analyst/Special Agent in IRS-CI
3 headquarters in the Financial Crimes section, Washington D.C. As a Senior Analyst in Financial
4 Crimes, I oversaw and managed several program areas to include the Virtual Currency program
5 and I was the IRS-CI liaison at the Financial Crimes Enforcement Network ("FinCEN").

6 2. In this capacity as a program manager for IRS-CI's Virtual Currency investigative
7 efforts; I made policy recommendations to senior leadership within IRS-CI, I provided guidance
8 to Special Agents in the field who were working cases with a virtual currency nexus, and I
9 provided virtual currency training for IRS-CI and other law enforcement agencies at the
10 international, federal, state and local levels.

11 3. As the FinCEN liaison for IRS-CI, I was the sole IRS management official
12 responsible for IRS-CI's strategic plan as it relates to the criminal enforcement of the Bank
13 Secrecy Act ("BSA") and coordinated with IRS civil on civil regulatory enforcement matters.

14 4. Before joining IRS-CI, I served 11 years as an Internal Revenue Agent assigned to
15 a specialized branch called Special Enforcement Program ("SEP"). SEP's primary focus is to
16 conduct civil detailed examinations where fraud may be present. These civil examinations were
17 conducted on both legal and illegal enterprises.

18 5. During my government service with Internal Revenue Service, I earned a Bachelor
19 of Business Administration with a focus in accounting from the Illinois Institute of Technology.

20 6. Kugelman Law, P.C. retained the Black Raven Advisory Group LLC on May 20,
21 2021 to assist in a matter that may involve the recovery of Bitcoin.

22 7. In support of this declaration, I have reviewed the following documents or sources
23 of information, these include but are not limited to: Complaint for Forfeiture filed 11/05/2020
24 Case 3:20-CV-07811, Verified Claim and Statement of Interest of Ilija Mr. Matusko filed
25 07/02/2021 Case CV 20-7811, Motion to Strike the Verified Claimant Ilija Matusko filed
26 07/29/2021 Case 3:20-CV-07811, Reply In Support Of Motion To Strike The Claims Of
27 Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred
28 Holdings, LLC filed 08/24/2021 Case No. CV 20-7811 RS, Declaration of Jeremiah Haynie,

Attachment A, Notice of Motion and Motion To Strike The Verified Claim of Claimant Ilija Mr. Matusko, Case 3:20-vc-07811 filed 07/29/2021, Declaration Of Jeremiah Haynie In Support Of United States' Reply In Support Of Motion To Strike The Claims Of Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case No. CV 20-7811 RS filed 08/24/2021, transcripts of sworn testimony of Former FBI Special Agent Ilhwan Yum January 29, 2015 – *United States of America v. Ross William Ulbricht*, Silk Road wiki web page, Sealed Ex Parte Application for a Second Post-Complaint Protective Order dated October 24, 2013, Declaration of Ilija Mr. Matusko dated August 26, 2021, bank statements, deposit receipts, various articles relating to the Silk Road Marketplace written by journalists, various academic papers written by scientists and university professors, the blockchain and certain transactions within the blockchain, historical prices of Euros, historical prices of Bitcoin, articles related to the fungibility of crypto currency, the Internal Revenue Service Internal Revenue Manual, the U.S. Department of Justice – Criminal Division – Money Laundering and Asset Recovery Section – Asset Forfeiture Policy Manual 2021, and other open-source information available via the internet.

SILK ROAD MARKETPLACE USER PROFILE “hanson5”

8. In approximately December of 2011, Ilija Matusko (“Mr. Matusko”) accessed the Silk Road Market and created a new user profile under the moniker of “hanson5”. The final stage in opening the user profile on the Silk Road Marketplace was to fund the profile with Bitcoin(s). Mr. Matusko clicked on an area in the Silk Road Marketplace user interface that provided information on how to fund the respective user profile. Mr. Matusko was provided a Bitcoin Address by the Silk Road Marketplace to fund the profile.

9. In December of 2011, Mr. Matusko purchased 48 Bitcoin from a third party, who also resided in the Federal Republic of Germany (Germany), for approximately €150 Euros. Mr. Matusko thereafter transferred these 48 Bitcoin to the Silk Road Marketplace Bitcoin wallet. “A copy of the Silk Road server when it was seized in October 2013 showed that the hanson5

1 account received 47.52 Bitcoin in December 2011.”¹

2 10. At no time during the period that the “hanson5” user profile was in existence did
3 Mr. Matusko purchase anything illegal or legal on the Silk Road Marketplace. This has been
4 acknowledged by the government: “Although the government does not question Mr. Matusko’s
5 assertion that he did not purchase any items from Silk Road using his hanson5 account,...”².

6 11. Attached as Exhibit 1 is a graphical representation of the purchase of Bitcoin(s) by
7 Mr. Matusko from a third party and the subsequent transfer of the 48 Bitcoin(s) from the third
8 party’s Bitcoin wallet to Mr. Matusko’s Bitcoin wallet. Included with this graphical
9 representation is the analysis that was performed by your declarant and source documents utilized
10 for the analysis and to reconstruct the respective transaction(s).

11 12. From my analysis, education, training, and experience as a professional in private
12 practice, as a law enforcement officer and senior leader with the IRS-CI I was able to conclude
13 the following:

14 13. That the account balance in Mr. Matusko’s bank account were from legal sources,
15 specifically from his receipt of unemployment compensation from Germany.

16 14. The funds (€150) used by Mr. Matusko to purchase the 48 Bitcoin from the third
17 party were from legal sources, specifically from his receipt of unemployment compensation from
18 Germany.

19 15. The character of the 48 Bitcoin after the completed purchase and subsequent
20 transfer from the third party’s Bitcoin wallet to Mr. Matusko’s Bitcoin wallet are legal source
21 Bitcoin.

22 16. The character of the 48 Bitcoin after the transfer from Mr. Matusko’s Bitcoin
23 wallet to the Silk Road Market wallet remained legal source Bitcoin.

24 17. The character of the “hanson5” 48 Bitcoin remained legal source Bitcoin for the
25 entire life of the Silk Road user profile of Mr. Matusko under the moniker of “hanson5”.

26 18. That only the actions of Mr. Matusko can change the character of the “hanson5”

27 ¹ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 6 ¶ 12:10-11

28 ² Notice of Motion and Motion To Strike The Verified Claim of Claimant Ilija Matusko, Case 3:20-vc-07811-RS,
filed 07/29/2021 at 20:15-16

1 48 Bitcoin. These are referred to as “downstream transactions”. At no time did Mr. Matusko
 2 purchase any item(s), legal or illegal on the Silk Road website. Because there were no purchases
 3 by Mr. Matusko through the “hanson5” profile on the Silk Road Marketplace, there were no
 4 “downstream transactions” that would have changed the character of the “hanson5” 48 Bitcoin.

5 19. That the transfer of Bitcoin to fund a Silk Road Marketplace user profile by itself
 6 is not illegal.

7 20. That maintaining a profile credit in a Silk Road Marketplace user profile by itself
 8 is not illegal.

9 21. That the Bitcoin(s) that are maintained on the Silk Road Marketplace Bitcoin
 10 wallet become proceeds of illegal activity when the Silk Road Marketplace user purchases goods
 11 or services from a vendor that are illegal in nature and the transaction has been completed. The
 12 completed transaction is considered the downstream transaction.

13 22. In the case of the Silk Road Marketplace, the illegal transaction is completed when
 14 the Bitcoin are released by the settlement agent (Mr. Ross Ulbricht, hereinafter “Ulbricht”) to the
 15 Silk Road Marketplace vendor. It is at this point that the Bitcoin become proceeds of the illegal
 16 activity. Any commission(s) earned by Ulbricht that are derived from the sale of illegal items on
 17 the Silk Road Marketplace are also considered proceeds of illegal activity.

18 23. Individuals and groups involved in illegal activity attempt to hide their illegal
 19 activities and attempt to disguise financial transactions, specifically; sources, uses and profits of
 20 funds directly or indirectly tied to illegal activity. From my analysis in Exhibit 1, Mr. Matusko
 21 did not make any effort to hide the purchase of the Bitcoin. In fact, Mr. Matusko did the complete
 22 opposite. He clearly documented the purchase of Bitcoin by notating “48 BTC Ilija” when he
 23 authorized a transfer of €150 (debit) from his bank to the third-party’s bank account. This Bitcoin
 24 purchase transaction is also clearly documented in the counter transaction (credit) of €150 with
 25 the third-party’s financial institution. Again, the purpose of the transaction is clearly notated on
 26 the financial institution’s documents as “48 BTC Ilija”.

27 **SILK ROAD MARKETPLACE OVERVIEW**

28 24. From my education, training, and experience as a professional in private practice,

1 as a law enforcement officer, as a senior leader with the IRS-CI, and through open-source
 2 information available via the internet, I know the following:

3 25. The Silk Road Marketplace was a darknet marketplace where both unlawful and
 4 lawful goods and services were sold by Silk Road Marketplace vendors and purchased by Silk
 5 Road Marketplace purchasers. A majority of these sales were illegal items, such as illicit
 6 narcotics, and these purchases and sales were nefarious in nature. But there were some sales of
 7 legal goods on the Silk Road Marketplace³ and there were other purchases that may have
 8 involved illegal items, but the nature of the purchases may not have been nefarious in nature. An
 9 example of this is shown below.

10 26. A simple Google search for “Silk Road Marketplace” will reveal numerous articles
 11 and academic papers written by journalist, scientists and university professors, all of whom may
 12 have created user profiles on the Silk Road Marketplace; funded these user profiles with Bitcoin;
 13 made purchases on the Silk Road Marketplace; gathered data through daily web crawls of the Silk
 14 Road Marketplace; or used other techniques to gather data on the Silk Road Marketplace. The
 15 data that was gathered throughout this process were used to write journalistic articles⁴ or
 16 academic articles that appeared in peer reviewed journals. These are examples of activity on the
 17 Silk Road Marketplace where the activity was not nefarious in nature.

18 27. “Silk Road was owned and operated by its creator Ross William Ulbricht, a/k/a
 19 “Dread Pirate Roberts,” a/k/a “DPR,” a/k/a “Silk Road”. Ulbricht controlled and oversaw all
 20 aspects of Silk Road. He maintained the computer infrastructure and programming code
 21 underlying the Silk Road website; he determined vendor and customer policies, including
 22 deciding what could be sold on the site; he managed a small staff of online administrators who
 23 assisted with the day-to-day operations of the site; and he alone controlled the massive profits
 24 generated from the operation of the business”⁵.

25 28. Ulbricht not only controlled the massive profits, but Ulbricht also controlled all

26 ³ [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)](https://en.wikipedia.org/wiki/Silk_Road_(marketplace))

27 ⁴ Gawker published what is thought to be one of the first articles on the Silk Road Marketplace which may have led
 to an increase notoriety of the darknet site, and it may have drawn the attention of U.S. Law Enforcement, including
 the attention of Senator Charles E. Schumer, United States Senator for New York.

28 ⁵ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 3 ¶ 6:10-16

1 Bitcoin transactions within the Silk Road Market sphere because Ulbricht alone controlled the
 2 Silk Road Market Bitcoin wallet. Ulbricht controlled the private key(s) and the public key(s)
 3 (Bitcoin addresses) of the Silk Road Market Bitcoin wallet and thereby maintained dominion and
 4 control of the Silk Road Market Bitcoin wallet. “A wallet is a collection of private keys and
 5 corresponding addresses. It is typically under the control of a single private individual or
 6 service.”⁶ In this case the single person who controlled the Silk Road Marketplace wallet was
 7 Ulbricht.

8 29. Ulbricht through the Silk Road Marketplace was a settlement agent.^{7,8} This
 9 provided a level of trust between vendors and purchasers.

10 30. When dealing with the sale or purchase of illegal items, especially illegal
 11 narcotics, there is always a level of mistrust between all parties. Ulbricht through the Silk Road
 12 Marketplace provided a platform where this mistrust may have been lessened.

13 31. As the government clearly established in the criminal trial of Ulbricht, he and only
 14 he controlled all aspects of the Silk Road Marketplace to include the Silk Road Marketplace
 15 Bitcoin wallet. This control of the Silk Road Marketplace Bitcoin wallet is critical. It established
 16 trust between vendors and purchasers, and it assured that Ulbricht generated and “controlled
 17 massive profits”⁵ from this enterprise.

18 **OVERVIEW OF BITCOIN WALLET PUBLIC KEYS AND PRIVATE KEYS**

19 32. From my education, training, and experience as a professional in private practice,
 20 as a law enforcement officer and senior leader with IRS-CI, and through open-source information
 21 available via the internet, I know the following:

22 33. A Bitcoin wallet is comprised of two keys: a private key and a public key
 23 (product(s) of the public key are Bitcoin addresses).

24 34. The wallet uses the private key to create a public key, then it “hashes” the public
 25

26 ⁶ Declaration Of Jeremiah Haynie In Support Of United States’ Reply In Support Of Motion To Strike The Claims Of
 Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case No.
 CV 20-7811 RS filed 08/24/2021 at 7 ¶ 22:26-27

27 ⁷ A settlement agent is an independent party who helps complete a transaction between a buyer and a seller and
 settles any disputes between the parties.

28 ⁸ Graphic depiction labeled “Government Exhibit 113A” Notice of Motion and Motion To Strike The Verified Claim
 of Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/21 at 21:1-13

1 key to generate a Bitcoin address. The Bitcoin address serves as a “destination address” that can
 2 be shared with anyone so that Bitcoin can be received by the specific Bitcoin address. Anyone
 3 with a Bitcoin wallet can receive Bitcoin. The sender of Bitcoin only needs to know the
 4 “destination address” also known as the Bitcoin address. It is this Bitcoin address that appears on
 5 the blockchain. To receive Bitcoin, the sender only needs to know the Bitcoin address of the
 6 recipient.

7 35. A Bitcoin wallet can have as many Bitcoin addresses as the Bitcoin wallet user
 8 wishes: “you could create hundreds, thousands of addresses in one wallet file”⁹ (Attached as
 9 Exhibit 2 is a copy of the transcript of sworn testimony of former FBI Special Agent Ilhwan
 10 Yum, January 29, 2015). “Users can operate multiple Bitcoin addresses at any given time and can
 11 use a unique Bitcoin address for each transaction.”¹⁰

12 36. The private key is a critical part of keeping a Bitcoin wallet secure. Each Bitcoin
 13 wallet’s private key is a very secure passcode that is used to lock and unlock the Bitcoin wallet so
 14 that the Bitcoin wallet owner can send or spend the Bitcoin that reside in the Bitcoin wallet. The
 15 only way to send or spend Bitcoin from a wallet is to have access to the private key(s). “Only the
 16 holder of a Bitcoin address’ private key can authorize transfers of Bitcoin from that address to
 17 other Bitcoin addresses.”¹¹ The person who controls the private key(s) is the person who
 18 controls the Bitcoin wallet.

19 37. The importance of the private key and who controls the wallet is illustrated by the
 20 government in three examples¹²: the government seizure of the Silk Road Marketplace Bitcoin
 21 wallet in or about October 2, 2013, and two instances in which Bitcoin were stolen from the Silk
 22 Road Marketplace Bitcoin wallet.

23 38. From my education, training, and experience as a professional in private practice,
 24 and as a law enforcement officer and senior leader with IRS-CI, I know that the seizures and/or
 25

26 ⁹ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1669:12-15

27 ¹⁰ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 7 ¶15:7-8

28 ¹¹ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 7 ¶15:6-7

¹² Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 4 ¶ 8, and at 5 ¶ 9-10

1 thefts were accomplished because the government, Individual X, and former U.S. Secret Service
 2 Special Agent Shaun Bridges accessed the private key(s) which controlled the Silk Road
 3 Marketplace Bitcoin wallet. The person(s) who has access to the private key(s) can unlock a
 4 Bitcoin wallet and can send or spend the Bitcoin in the Bitcoin wallet.

5 **FUNGIBILITY OF BITCOIN**

6 39. From my education, training, and experience as a professional in private practice,
 7 as a law enforcement officer, senior leader with IRS-CI, and other open-source information
 8 available via the internet, I know the following:

9 40. That a feature of currencies, commodities and certain crypto currencies (like
 10 Bitcoin) is fungibility.^{13 14}

11 41. Meaning that units of the currency, commodity or crypto currency are
 12 interchangeable. Fungibility is a core pillar of any currency, commodity, or crypto currency (like
 13 Bitcoin), that will be used as a means of exchange that is going to be widely used for daily
 14 transactions. It establishes that the good or commodity is reliable to be used on a consistent basis
 15 as a means of exchange.¹⁵

16 42. For example, the U.S. one-dollar bill; there are a great number of U.S. one-dollar
 17 bills in circulation, every U.S. one dollar bill is worth the same, and is interchangeable with any
 18 other U.S. one dollar bill. The same is true for U.S. five, ten, twenty, etc... dollar bills.

19 43. Some examples of items that are fungible: fiat currencies, Bitcoin, bonds, shares,
 20 precious metals, and sweet/light crude oil.

21 44. Some examples of items that are non-fungible include: art work, real estate,
 22 people, diamonds (unique in size, shape/cut, brilliance, color and grade), digital non-fungible-
 23 goods (NFGs) such as crypto kitties¹⁶, which are a one-of-a-kind digital pets.

24 45. Bitcoin(s) meets the definition of fungibility and is fungible in nature. Bitcoin are
 25 interchangeable, uniform, substitutable and equivalent in nature and therefor fungible.

26 ¹³ <https://www.investopedia.com/terms/f/fungibility.asp> - Investopedia.com defines fungibility as "Fungibility is the
 27 ability of a good or asset to be interchanged with other individual goods or assets of the same type."

¹⁴ Article 415 of the NAFTA defines fungible goods as "Fungible goods are goods that are interchangeable for
 28 commercial purposes, and have essentially identical properties."

¹⁵ <https://www.worldcryptoindex.com/fungibility-explained/>

¹⁶ <https://www.cryptokitties.co>

46. For example, if two people exchanged one Bitcoin for another, there would be no loss of value and neither party would be better off than the other. That is because there is no value distinction between any two Bitcoin. This is the definition of fungible. Just as one \$20 bill is just as valuable as another \$20 bill, 1 Bitcoin is just as valuable as another 1 Bitcoin.

SILK ROAD MARKETPLACE BITCOIN WALLET

47. Ulbricht maintained the Bitcoin server which contained the Bitcoin wallet¹⁷ for the Silk Road Marketplace. That Bitcoin wallet was in Iceland. The Silk Road Marketplace Bitcoin wallet had a great number of Bitcoin addresses (destination addresses) associated with it: 2,105,527 Bitcoin addresses¹⁸ to be exact.

48. “Upon registering an account with Silk Road, users were assigned a Bitcoin address. Bitcoin sent to the user’s Bitcoin address was credited to the user’s account”.¹⁹

49. From my education, training, and experience as a professional in private practice, as a law enforcement officer, and senior leader with IRS-CI, I know the following:

50. That the Silk Road Marketplace Bitcoin wallet that was controlled by Ulbricht was composed of private key(s) to keep it secure, and within the wallet were 2,105,527 Bitcoin addresses.

51. That the unique Bitcoin address that was assigned to the Silk Road Marketplace user was created by the Silk Road Marketplace Bitcoin wallet.

52. That the 2,105,527 Bitcoin addresses represent Bitcoin addresses that were assigned (at least in part) to users of the Silk Road Marketplace when they created a profile.

53. That an important feature of any Bitcoin wallet is the ability to create and manage multiple Bitcoin addresses. The ability to create and assign a unique Bitcoin address to each user of the Silk Road Marketplace was a key internal control; it allowed Ulbricht to easily track all Bitcoin(s) sent to the Silk Road Marketplace Bitcoin wallet and associate each respective Bitcoin(s) transfer with a specific Silk Road Marketplace user.

54. Ulbricht “controlled and oversaw all aspects of Silk Road”⁵ and this included the

¹⁷ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1656:12-18.

¹⁸ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1685:3

¹⁹ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 3 ¶ 7:26-27

1 Silk Road Marketplace Bitcoin wallet private key(s).

2 55. Ulbricht's control of the Silk Road Marketplace Bitcoin wallet private key(s) was
3 another critical internal control; as a settlement agent, Ulbricht needed control of the Silk Road
4 Marketplace wallet in the event of a dispute between a Silk Road Marketplace vendor and a Silk
5 Road Marketplace purchaser. This level of oversight also ensured that Ulbricht "alone controlled
6 the massive profits generated from the operation of the business"⁵. These profits that Ulbricht
7 controlled were commissions from all sales on the Silk Road Marketplace.

8 56. At no time did users of the Silk Road Marketplace have access to the private
9 key(s) of the Silk Road Marketplace Bitcoin wallet. Users only knew the Bitcoin address that
10 were assigned to their respective profile.

11 57. Only Ulbricht could send or spend Bitcoin from the Silk Road Marketplace
12 Bitcoin wallet, because only he had access to and controlled the private key(s).

13 **SEIZURE OF SILK ROAD MARKETPLACE BITCOIN WALLET**

14 58. The government was able to identify a server in Iceland that contained the Silk
15 Road Marketplace Bitcoin wallet and all the Bitcoin that resided in this wallet.²⁰

16 59. On or about October 2, 2013²¹ the government seized the Silk Road Marketplace
17 Bitcoin wallet that was located in Iceland. During this same U.S. Law Enforcement action, the
18 government gained control of the Silk Road Marketplace Bitcoin wallet private key(s), accessed
19 the Silk Road Marketplace Bitcoin wallet, and seized all of the Bitcoin that resided in the Bitcoin
20 wallet.²²

21 60. This U.S. Law Enforcement action in Iceland was a challenging, well-coordinated
22 operation that had specific goals.²³

23 61. One of these goals was to seize all the Bitcoin from the Silk Road Market Bitcoin
24 wallet.²⁴

25 62. The operational goal of seizing the Bitcoin from the Silk Road Market Bitcoin
26

27 ²⁰ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1649:6-20

²¹ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1646:10-11

²² Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1650:25 and at 1651:1- 10

²³ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1646:14-20

²⁴ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1648:22-23

wallet involved the following steps:

- (1) Go to the data center in Iceland with Icelandic Police²⁵
- (2) Locate the Silk Road Marketplace servers in the Icelandic data center²⁶
- (3) Examine the Silk Road Marketplace server to assess how it was set up²⁷
- (4) Turn off the Silk Road Marketplace server and seize the duplicate server hard drive as the true, best original evidence²⁸
- (5) After turning off the server, assess if the Silk Road Marketplace was offline²⁹
- (6) Turn the Silk Road Marketplace server back on³⁰ to create a ruse³¹
- (7) Assess if the Silk Road Marketplace was back online³²
- (8) Turn off the “update process”³³ to complete the ruse; and finally
- (9) Access the Silk Road Marketplace Bitcoin wallet that was on the other server³⁴ (the Bitcoin server) and seize/transfer the Silk Road Marketplace user’s³¹ Bitcoin to a government-controlled Bitcoin wallet.³⁵

63. The ruse to deceive the Silk Road Market user(s) who concurrently might have been viewing the marketplace or signed into their Silk Road Marketplace user profile, was devised for one purpose: disguising the users Bitcoin(s) credit on the Silk Road Marketplace user interface. As stated in the transcript of the Sworn testimony of Former FBI Special Agent Ilhwan Yum, “we didn’t want to alert the users of the Silk Road Marketplace that their Bitcoin are being seized [emphasis added],” and “as I was seizing the Bitcoin, the users wouldn’t be aware that the balance of the Bitcoin on the Silk Road was depleting.”³⁶

64. The Bitcoin that were seized by the government from the Silk Road Marketplace Bitcoin wallet on or about October 3, 2013 belonged to the “users”³¹ of the Silk Road Marketplace.

\\

\\

²⁵ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1647:10-11

²⁶ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1647:13-15

²⁷ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1647:22-24

²⁸ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1648:4-6

²⁹ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1648:9-16

³⁰ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1648:16-17

³¹ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1650:11-12

³² Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1648:17-18

³³ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1650:18-20

³⁴ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1651:6-7, and at 1648:22-24

³⁵ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1650:25, and at 1651:1-10

³⁶ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1650:20-22

**U.S. GOVERNMENT SEIZURE OF APPROXIMATELY 69,370 BITCOIN FROM
1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx (1HQ3)**

65. The U.S. Government conducted an investigation into the movement of some Bitcoin from a Bitcoin address that was dormant, specifically Bitcoin address 1HQ3 and other Bitcoin address(s) associated with 1HQ3. The U.S. government describes the investigation and results of the investigation as follows:

66. “According to an investigation conducted by the Criminal Investigation Division of the Internal Revenue Service and the U.S. Attorney’s Office for the Northern District of California, Individual X was the individual who moved the cryptocurrency from Silk Road. According to the investigation, Individual X was able to hack into Silk Road and gain unauthorized and illegal access to Silk Road and thereby steal the illicit cryptocurrency from Silk Road and move it into wallets that Individual X controlled.”³⁷

67. “This pattern of withdrawals and the amount that was withdrawn was not typical for a Silk Road user. Specifically, a review of other withdrawals from Silk Road revealed Bitcoin amounts that were mostly less than 100 Bitcoin. These 54 transactions were not noted in the Silk Road database as a vendor withdrawal or a Silk Road employee withdrawal and therefore appear to represent Bitcoin that was stolen from Silk Road.”³⁸

68. “In fact, the BTC (Bitcoin) Individual X stole came from the general pool of Silk Road Bitcoin and not from any particular user accounts, meaning that no user balances were impacted by the hack.”³⁹

69. The government has affirmatively concluded that the Bitcoin from this theft originated from the Silk Road Marketplace. “I was able to determine that the ultimate source of the funds in 1HQ3 originated from addresses managed by the same entity: the Silk Road marketplace.”⁴⁰

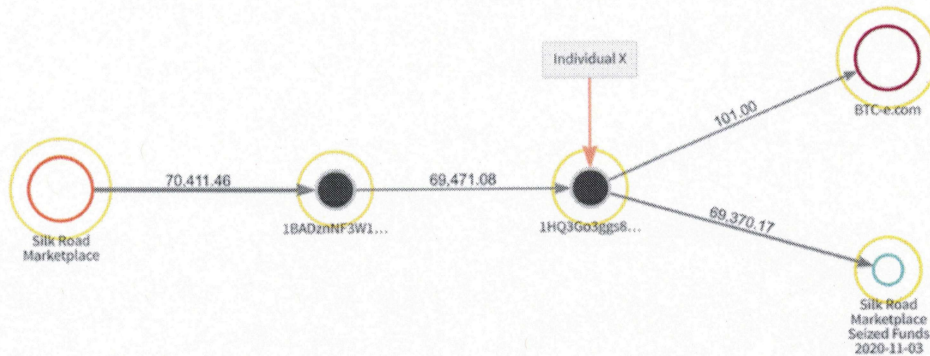
³⁷ Complaint for Forfeiture – USA, Plaintiff v. Approximately 69,370 bitcoin, Case 3:20-CV-07811-VC filed November 5, 2020 at 5 ¶ 22

³⁸ Complaint for Forfeiture – USA, Plaintiff v. Approximately 69,370 bitcoin, Case 3:20-CV-07811-VC filed November 5, 2020 at 4 ¶ 16

³⁹ Notice of Motion and Motion To Strike The Verified Claim of Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 8:19-21

⁴⁰ Declaration Of Jeremiah Haynie In Support Of United States’ Reply In Support Of Motion To Strike The Claims Of Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case

70. Below is an image of a graphic representation⁴¹ of the theft by Individual X that shows and establishes that the theft was from the Silk Road Marketplace. This graphic representation was created by the third-party Bitcoin attribution company that was utilized by the government in this investigation and seizure.



71. The government in a declaration used a similar graphic representation as above and provide an explanation: “The series of transactions begins on the left side of Exhibit 1, when on May 6, 2012, Individual X, without authorization, transferred 70,411.46 BTC from Silk Road to two Bitcoin addresses Individual X controlled, 1BAD and 1BBq.”⁴² Again, the government clearly established that the theft on or about May 6, 2012 originated from the Silk Road Marketplace Bitcoin wallet.

72. The government conducted an extensive analysis of the originating Bitcoin addresses that were affected by the theft that occurred on or about May 6, 2012 and concluded the following: “Individual X sent the stolen Bitcoin to 1BAD & 1BBq in 54 separate transactions. Each of those transactions was funded by multiple Bitcoin addresses associated with Silk Road. In total, 1BAD & 1BBq were funded by approximately 3,056 sending addresses.”⁴³

No. CV 20-7811 RS filed 08/24/2021 at 5 ¶ 15:26-27

⁴¹ <https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020>

⁴² Declaration Of Jeremiah Haynie In Support Of United States’ Reply In Support Of Motion To Strike The Claims Of Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case No. CV 20-7811 RS filed 08/24/2021 at 6 ¶ 16:1-3

⁴³ Declaration Of Jeremiah Haynie In Support Of United States’ Reply In Support Of Motion To Strike The Claims Of Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case No. CV 20-7811 RS filed 08/24/2021 at 8 ¶ 24:7-9

1 73. This extensive analysis concluded the following: "Of the 3,056 sending addresses,
2 3,014 were deposit addresses for Silk Road users."⁴⁴

3 74. From my education, training, and experience as a professional in private practice,
4 as a law enforcement officer and senior leader with IRS-CI, and based on documents and other
5 sources of information reviewed for this declaration, I know the following:

6 75. That the Bitcoin that were seized by the government in or about October 2, 2013
7 came from the Silk Road Marketplace Bitcoin wallet.

8 76. That the Bitcoin seized by the government in or about October 2, 2013 were the
9 property of the Silk Road Marketplace users³¹.

10 77. I know that the theft/illegal transfer of Bitcoin by Individual X on or about May 6,
11 2012 came from the Silk Road Market Bitcoin wallet.

12 78. That the Bitcoin stolen by Individual X originated from the Silk Road Marketplace
13 Bitcoin wallet and that the Bitcoin in this wallet was the property of the Silk Road Marketplace
14 users³¹.

15 79. I know that that if there is an authorized or unauthorized transfer of Bitcoin from
16 any Bitcoin wallet, that this transfer will reduce the total number of Bitcoin in the respective
17 wallet by the amount of the transfer.

18 80. That the seizure by the government in or about October 2, 2013 affected the total
19 credit of the Silk Road Marketplace Bitcoin wallet, by "a little over 20,000 Bitcoin".⁴⁵

20 81. I know that the theft/illegal transfer of Bitcoin in or about May 6, 2012 by
21 Individual X affected the total credit of the Silk Road Marketplace wallet, by exactly 70,411.46
22 Bitcoin.

23 82. I know that the Bitcoin in the Silk Road Marketplace wallet is the property of the
24 Silk Road Market users, to include Mr. Matusko.

25 **U.S. LAW ENFORCEMENT PRE-SEIZURE PLANNING**

26 83. From my education, training, and experience as a professional in private practice,

27 ⁴⁴ Declaration Of Jeremiah Haynie In Support Of United States' Reply In Support Of Motion To Strike The Claims
28 Of Claimants Battle Born Investments Company, LLC, First 100, LLC And 1st One Hundred Holdings, LLC Case
 No. CV 20-7811 RS filed 08/24/2021 at 8 ¶ 24:11-12

⁴⁵ Exhibit 2 Transcript Sworn testimony of Former FBI Special Agent Ilhwan Yum at 1651:9-10

1 as a law enforcement officer, and senior leader with the IRS-CI, I know the following:

2 84. That the Department of Justice – Asset Forfeiture and Money Laundering Section
3 now known as the Money Laundering and Asset Recovery section provides guidance in money
4 laundering investigations and in seizure/forfeiture matters to the appropriate United States
5 Attorney’s Office and to U.S. Law Enforcement. This guidance includes manuals and other aid to
6 assist Assistant United States Attorney’s and U.S. Law Enforcement in money laundering
7 investigations and in seizure/forfeiture matters.

8 85. Attached as Exhibit 3 is an aide that is titled “Basic Criminal Forfeiture Checklist”
9 and is often provided to Assistant United State Attorney’s and U.S. Law Enforcement.

10 86. The first five steps as outlined in this aide are:

- 11 (1) Identify assets that are subject to forfeiture
12 (2) Determine ownership of the assets
13 (3) Determine the net value of the assets
14 (4) Determine the statutory basis for the forfeiture
15 (5) Identify and investigate possible third-party interests [emphasis added].

16 87. Attached as Exhibit 4 is Internal Revenue Service – Internal Revenue Manual
(IRM) Part 9. Chapter 7. Section 4. – Asset Seizure and Forfeiture -Pre-Seizure Planning.⁴⁶

17 88. IRM 9.7.4.1 (2) states “Pre-seizure planning should occur, in both civil and
18 criminal seizure and forfeiture actions, prior to the actual physical seizure of property, and prior
19 to the filing of a civil judicial forfeiture complaint or an indictment with a forfeiture count or
20 allegation.”

21 89. IRM 9.7.4.2 (1) states “The Assistant United States Attorney (AUSA) is
22 responsible for ensuring that proper and timely pre-seizure planning occurs in civil judicial and
23 criminal forfeiture actions. In administrative forfeiture actions, the Asset Forfeiture Coordinator
24 (AFC) has this responsibility.”

25 90. IRM 9.7.4.2 (2) states “Although the AUSA may be ultimately responsible for pre-
26 seizure planning in civil judicial and criminal forfeiture actions, the AFC is responsible for
27 initiating the pre-seizure planning process set forth in this section and ensuring that they are

28 ⁴⁶ https://www.irs.gov/irm/part9/irm_09-007-004

1 followed in all seizure and forfeiture actions.”

2 91. This pre-seizure planning by the Special Agent and the Asset Forfeiture
3 Coordinator includes but is not limited to: identifying and investigating the ownership interest(s)
4 in those who may have an interest in the property that is being seized.

5 92. Attached as Exhibit 5 is the Money Laundering and Asset Recovery section Asset
6 Forfeiture Policy Manual 2021.⁴⁷

7 93. Asset Forfeiture Policy Manual 2021, Chapter 1 Section C.2 Seizure Planning
8 Overview, states, “seizure planning consists of anticipating issues and making fully informed
9 decisions concerning what property should be seized or restrained, how and when it should be
10 seized or restrained, and, most importantly, whether the property should be forfeited at all.”

11 94. Chapter 1 Section C.2 Seizure Planning Overview continues “Seizure planning
12 discussions should answer at least the following questions, depending on asset type and
13 circumstance: What is being seized, who owns it, and what are the liabilities against it [emphasis
14 added]? Determine the full scope of the seizure to the extent possible. For example, if a house is
15 being seized, will the contents also be seized? If a business is being seized, are the buildings in
16 which it operates, the property upon which it is located, the inventory of the business, and the
17 operating or other bank accounts, accounts receivable, accounts payable, etc., also to be seized?
18 All ownership interests and any existing or potential liabilities in each asset must be identified to
19 the extent possible [emphasis added].”

20 95. Asset Forfeiture Policy Manual 2021, Chapter 4 Section I. Pre-forfeiture
21 Considerations states: “All real property pre-seizure procedures rely upon the accurate calculation
22 of value and the identification of ownership interests [emphasis added].”

23 96. Since at least on or about October 2, 2013 the government knew that it was
24 planning to seize the assets of the Silk Road Marketplace users. Each Silk Road Marketplace user,
25 like Mr. Matusko, who had a profile credit at the time of the government seizure on or about of
26 October 2, 2013, may have an ownership interest in Bitcoin seized by the government in or about
27 October of 2013 and again in or about November of 2020.

28
⁴⁷ <https://www.justice.gov/criminal-mlars/publications>

1 97. As demonstrated in the government's response to the Mr. Matusko claim, the
2 government maintains a copy of Silk Road Marketplace server. At the will of the government,
3 they can access and check users profiles, as they did with the Mr. Matusko "hanson5" profile. "A
4 copy of the Silk Road server when it was seized in October 2013 showed that the hanson5
5 account received 47.52 Bitcoin in December 2011. The hanson5 Silk Road account had the same
6 balance when the server was seized in October 2013."⁴⁸

7 98. The government has always had the ability to export all Silkroad Marketplace user
8 data in an attempt to identify third parties who may have a financial interest in the seizure that
9 occurred in or about October 2, 2013, and again in this seizure that occurred in or about
10 November of 2020. "When the government seized the Silk Road website in 2013, it preserved its
11 servers, which contain the entire transaction history and users of the website."⁴⁹

12 99. Each Silk Road Marketplace user, to include Mr. Matusko, who had a profile
13 credit at the time of the government seizure in October of 2013 is a potential third party who may
14 have a financial interest in the Bitcoin seized in October of 2013 and again in November of 2020.

15 **BITCOIN ADDRESS OWNER'S IDENTITY & INFORMATION AVAILABLE TO U.S.**

16 **LAW ENFORCEMENT**

17 100. "While a Bitcoin address owner's identity is generally anonymous within the
18 blockchain (unless the owner chooses to make information about the owner's Bitcoin address
19 publicly available), investigators can often use the blockchain to identify the owner of a particular
20 Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin
21 transaction, investigators can trace transactions to, among other recipients, virtual currency
22 exchanges."⁵⁰

23 101. From my education, training, and experience as a professional in private practice,
24 as a law enforcement officer, senior leader with the IRS-CI, and through open-source information
25 available via the internet I know the following:

26 ⁴⁸ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
27 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 6 ¶ 12:10-12

28 ⁴⁹ Reply In Support Of Motion To Strike The Claims Of Claimants Battle Born Investments Company, LLC, First
100, LLC And 1st One Hundred Holdings, LLC filed 08/24/2021 Case No. CV 20-7811 RS at 6:10-11

⁵⁰ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 7 ¶ 17.

1 102. That U.S. Law Enforcement has access to certain information that is not available
2 to the public when it comes to identifying Bitcoin transactions and Bitcoin address owner(s). This
3 information includes but is not limited to the following:

4 103. Reports that are mandated by FinCEN, due to FinCEN's regulatory authority
5 under Title 31 and FinCEN's authority over crypto currency exchanges that operate as money
6 service business in the United States. These reports that are filed with FinCEN are made available
7 to U.S. Law Enforcement almost immediately upon filing and typically provide the following: a
8 narrative as to suspect activity, the identity of the owner of the exchange account(s), physical
9 address, social security number, e-mail addresses, other identifying information, IP addresses
10 used in transaction(s) and the Bitcoin address utilized by the individual(s). These reports are
11 available to U.S. Law Enforcement through FinCEN. They can be easily accessed at any time by
12 U.S. Law Enforcement by logging into the FinCEN system containing these reports. In fact, the
13 Internal Revenue Service receives weekly, if not more frequent, downloads of these reports and
14 other reports from FinCEN that are integrated into a very powerful software program that is
15 utilized by IRS-Criminal Investigation.

16 104. That U.S. Law Enforcement maintains copies of servers from past U.S. Law
17 Enforcement actions. A simple Google search of "IRS-Criminal Investigation Cyber Crime Unit"
18 will reveal numerous articles, podcasts, presentations by Cyber Crime Unit Special Agents. That
19 search will also show that IRS-CI has taken the lead and assisted on many darknet investigations,
20 including those of child exploitation sites, darknet marketplaces, unlicensed cryptocurrency
21 money exchangers, tumbler services, seizure of terrorist funds and more. Each of these types of
22 criminal investigations are serious enough to result in a U.S. Law Enforcement action(s)
23 involving the seizure of the servers of these illicit and in certain circumstances heinous criminal
24 acts. The data on these servers are invaluable to U.S. Law Enforcement as they link data from one
25 criminal matter to other criminal matters.

26 105. We know in this seizure of the approximate 69,370 Bitcoin that the government
27 utilized data from an unrelated criminal investigation, specifically, BTC-e⁵¹, to positively identify
28

⁵¹ Complaint for Forfeiture filed 11/05/2020 Case 3:20-CV-07811-VC at 5 ¶ 18

1 Individual X, who is known to the government.⁵² This data from the BTC-e servers tied
 2 Individual X to Bitcoin address 1HQ3 and provided key identifying information to make him
 3 known to the government. This is just one example of data from unrelated criminal cases that are
 4 warehoused with the IRS and other U.S. Law Enforcement.

5 106. Over the past six years the IRS has been issuing John Doe Summons to various
 6 crypto currency exchangers including but not limited to: Coinbase, Kraken, Circle, and other
 7 U.S.-based crypto currency exchangers. The data that the government has obtained, or will
 8 obtain, includes account holder information and transactional information for those who had
 9 \$20,000 or more in gross transactions. These U.S. domiciled exchangers must be registered with
 10 FinCEN as a money service business and as a result the must have a robust anti-money
 11 laundering (“AML”) program to be in compliance with FinCEN and the Bank Secrecy Act. A
 12 major part of any AML program is to “know your customer”. The account holder information
 13 and transaction information that these exchangers have provided or will provide to the IRS will be
 14 extremely valuable in identifying Bitcoin transactions and Bitcoin address owners.

15 107. IRS-Criminal Investigation utilizes extremely powerful software called Palantir to
 16 harvest raw data, to digest the raw data, to analyze the data, and to identify cryptocurrency
 17 patterns and connections.

18 108. “In 2020, law enforcement officers used a third-party Bitcoin attribution company
 19 to analyze Bitcoin transactions executed by Silk Road. From this review they observed 54
 20 transactions that were sent from Bitcoin addresses controlled by Silk Road, to two Bitcoin
 21 addresses: 1BADznNF3W1gi47R65MQs754KB7zTaGuYZ and
 22 1BBqjKsYuLEUE9Y5WzdbzCtYzCiQgHqtPN totaling 70,411.46 BTC (valued at approximately
 23 \$354,000 at the time of transfer).”⁵³ Since at least 2015⁵⁴, IRS-Criminal Investigation has utilizes
 24 the services of Chain Analysis for complex tracing of blockchain transactions, in addition to its
 25 analysis software and did so in this seizure.⁵⁵

26 109. The government, especially the IRS, has collected a great quantity of data in its

27 ⁵² Complaint for Forfeiture filed 11/05/2020 Case 3:20-CV-07811-VC at 5 ¶ 21

⁵³ Complaint for Forfeiture filed 11/05/2020 Case 3:20-CV-07811-VC at 4 ¶ 15.

28 ⁵⁴ <https://www.documentcloud.org/documents/3935924-IRS-Chainalysis-Contract.html>

⁵⁵ <https://blog.chainalysis.com/reports/silk-road-doj-seizure-november-2020>

1 efforts to identify owners of Bitcoin addresses and related transactions on the blockchain. The
 2 government also possesses very powerful software. With this data and the powerful data that the
 3 IRS has, the government can easily identify third parties who have an interest in these type of
 4 cases and seizures.

5 **DIRECT NOTICE OF SEIZURE**

6 110. From my education, training, and experience as a professional in private practice,
 7 as a law enforcement officer, senior leader with the IRS-CI, and through open-source information
 8 available via the internet I know the following:

9 111. That when a third party's interest in an asset that was seized by the government is
 10 discovered in the pre-seizure investigative phase or afterwards, the government must provide
 11 direct notice to this third party.

12 112. That at least one user and third party who may have had a financial interest in this
 13 seizure of approximately 69,370 Bitcoin was provided direct notice. "The government sent direct
 14 notice to Ulbricht in prison. Ulbricht is the only individual known to the government with a
 15 potential interest in the Defendant Property and is therefore the only person who received direct
 16 notice."⁵⁶

17 113. Ulbricht was a user and maintained a user profile on the Silk Road Marketplace.
 18 "The contents of the Silk Road web server included Ulbricht's own user account page, which
 19 reflected, among other things, his history of Bitcoin transactions on the site. Ulbricht's transaction
 20 history reflects that he received a continuous flow of Bitcoin into his Silk Road account. For
 21 example, on July 21, 2013 alone, Ulbricht received approximately 3,237 separate transfers of
 22 Bitcoin into his account. Virtually all of those transactions were labeled "commission" in the
 23 "notes" appearing next to them, indicating that the money represented commissions from Silk
 24 Road sales. Ulbricht's account page further displayed the total amount of Bitcoin deposited in his
 25 Silk Road account, which, as of July 23, 2013, equaled more than \$3.4 million."⁵⁷

26 114. Even though the Bitcoin credit in Ulbricht's Silk Road Marketplace user profile

27 ⁵⁶ Notice of Motion and Motion To Strike The Verified Claim of Claimant Ilija Matusko, Case 3:20-vc-07811-RS,
 filed 07/29/2021 at 16:13-15

28 ⁵⁷ Declaration of Jeremiah Haynie, Attachment A, Notice of Motion and Motion To Strike The Verified Claim of
 Claimant Ilija Matusko, Case 3:20-vc-07811-RS, filed 07/29/2021 at 3 ¶ 6:16-23

1 was proceeds from illegal activities, commission earned from the sale of illegal items, Ulbricht
2 was still provided direct notice.

3 115. I know that the 48 “hanson5” Bitcoin in Mr. Matusko’s user profile were legal
4 source Bitcoin.

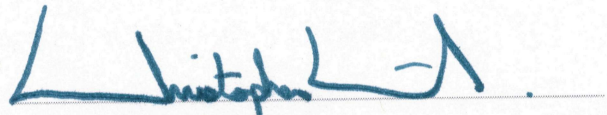
5 116. I know that Mr. Matusko did not engage in an illicit activity on the Silk Road
6 Marketplace.

7 117. I know that the Bitcoin in the Silk Road Marketplace wallet is the property of the
8 Silk Road Marketplace users³¹, to include Mr. Matusko and Ulbricht.

9 118. I know that Mr. Matusko did not receive direct notice from the government as a
10 third party who may have an interest in the assets seized in or about October 2, 2013, or in this
11 seizure of approximately 69,370 that occurred in or about November of 2020.

12 I declare under penalties of perjury under the laws of the United States of America that the
13 foregoing is true and correct to the best of my knowledge and belief.

14 Executed on this 26th day of August 2021, in Clifton, Virginia

15
16
17
18 

19 CHRISTOPHER WAJDA,
20 Managing Director
21 Black Raven Advisory Group LLC
22
23
24
25
26
27
28